부록 2-2

1.0

국가 망 보안체계 보안 가이드라인

정보서비스 모델 해설서

모델 2. 업무환경에서 생성형 AI 활용

2025. 9

국가정보원

NSR 국가보안기술연구소

부록 2-2

1.0

국가 망 보안체계 보안 가이드라인

정보서비스 모델 해설서

모델 2. 업무환경에서 생성형 AI 활용

2025. 9

국가정보원

NSR 국가보안기술연구소

국가 망 보안체계

보안 가이드라인

정보서비스 모델 해설서 - 모델 2. 업무환경에서 생성형 AI 활용

부록 2-2

문서이력

개정일	버전	내역	비고
2025.1.	Draft	「국가 망 보안체계 보안 가이드라인 – 정보서비스 모델 해설서」 발간	
2025.9.	1.0	「국가 망 보안체계 보안 가이드라인 – 정보서비스 모델 해설서 – 모델 2. 업무환경에서 생성형 AI 활용」 발간	모델별 분리

CONTENTS

CONTENTS

Table List

Figure List

제1장

정보서비스 모델 해설서 개요

제1절

정보서비스 모델 해설서 개요

1. 개요

본 해설서는 국가·공공기관에서 정보서비스[1] 구축·운영시 국가 망 보안체계(N2SF) 적용을 위한 보안 가이드라인 부록으로, 정보서비스 모델의 보안대책 수립을 위한 위협식별, 보안 요구사항 도출 및 보안통제 항목 선정 방법 제시를 목적으로 한다.

각급기관에서 구축·운영하고자 하는 정보서비스는 업무 환경 및 기관 특성에 따라 다른 형태로 구현되는 것이 일반적이지만, 다수 기관에서 생성형 AI, 외부 클라우드 서비스의 업무 활용 등 유사한 목적과 기능을 갖는 정보서비스의 구축이 이루어질 것으로 예상된다.

본 문서에서는 유사한 목적의 공통 정보서비스 모델을 도출하여 상위 수준에서 서비스 구조 및 구현 방법 등을 구체화하는데 참고할 수 있는 참조 모델을 제시한다. 각급기관에서 요구되는 정보서비스 모델을 정의하고 해당 모델에 적합한 보안대책 제시를 통해, 정보서비스 모델 구축·운용 시 필요한 보안대책 수립을 지원하고자 한다.

정보서비스 모델 해설서는 국가 망 보안체계 적용을 통해 변화하는 공공부문 주요 정보서비스 모델을 선정하여 보안 위협식별 및 그에 따르는 보안 요구사항 도출을 통한 보안 대책 수립에 초점을 맞추었으며, 각급기관이 해설서를 참조하여 보안대책을 적용 가능하도록 구성하였다.

1) 정보서비스는 업무정보를 이용해 특정 서비스를 제공하기 위해 하나 이상의 정보시스템으로 구성된 체계를 의미한다. 정보화 사업에서 정보시스템은 구축 및 운영의 대상이며, 정보시스템을 통해서 정보서비스를 제공하게 된다.

2. 문서 구조

본 문서는「업무환경에서 생성형 AI 활용」정보서비스 모델에 대해 설명하고 있으며, 2장은 정보서비스 개요, 위협식별, 보안대책 수립 등 총 3개의 절을 포함하고 있다. 2장에 대응하는 N2SF 단계/활동은 다음과 같다.

표 1-1 2장과 N2SF 단계/활동의 대응 관계

절	항	N2SF 단계	N2SF 활동명	세부 내용
제1절 정보서비스 개요	-	-	-	N2SF 정보서비스 개요 설명
제2절 정보서비스 보안위협 식별	1. 정보서비스 구성요소 분석	준비 (Prepare)	「활동-1-5」 정보서비스 식별	정보서비스를 구성하는 네트워크, 정보시스템, 업무정보 등 세부구성 분석, 사용 시나리오 정의 등
	2. 모델링 및 C/S/O 평가	위협식별 (Identify)	「활동-3-1」 모델링 및 C/S/O 평가	정보서비스의 각 구성요소(네트워크, 정보시스템 등)에 대한「위치-주체-객체」모델링 및 C/S/O 평가
	3. 보안원칙 적용		「활동-3-2」 보안원칙 적용	「정보 생산·저장」보안원칙 및「정보 이동」보안원칙 적용을 통하여 보안통제가 필요한 영역 확인
	4. 보안위협 식별		「활동-3-3」 보안위협 식별	정보서비스 구성에 기반하여 보안 위협 대상이 되는 정보시스템 및 네트워크 연계 지점, 서비스 위치를 파악하고 보안위협 요소 도출
제3절 보안 요구사항 및 보안대책	1. 이용자 단말	보안대책 수립 (Select)	「활동-4-1」 보안 요구사항 도출	정보서비스 구축·운영 과정에서 필요한 이용자 단말 보안 요구사항 정의 및 이를 기반으로 보안통제 항목 도출
			「활동-4-2」 보안통제 선택	
	2. 연계체계		「활동-4-1」 보안 요구사항 도출	기관 전산망과 네트워크 연계가 이루어지는 지점에 필요한 보안 요구사항 정의 및 이를 기반으로 보안통제 항목 도출
			「활동-4-2」 보안통제 선택	
	3. 생성형 AI 서비스		「활동-4-1」 보안 요구사항 도출	생성형 AI 서비스 활용 시 필요한 보안 요구사항 정의 및 이를 기반으로 보안통제 항목 도출
			「활동-4-2」 보안통제 선택	

제2절

정보서비스 모델 해설서 활용 방안

본 해설서는 각급기관이 국가 망 보안체계에 따라 획일적인 망 분리 정책에서 탈피하여 새로운 보안체계 하에서 AI·클라우드 등 신기술을 적용한 정보서비스를 도입하는 과정에서 도움이 될 수 있다. 2장에서 정보서비스에서 발생할 수 있는 보안 위협을 고려하여 보안통제 항목을 조정·반영한 결과의 예시를 제안하고 있다.

본 문서에서 제안하는 보안통제 항목은 절대적인 기준이 아닌 검토 사항으로 기관의 특성에 맞게 유연하게 적용할 필요가 있다. 즉, 본 문서에서 제시하는 보안통제 항목을 모두 구현해야 한다거나 제시되지 않은 보안통제 항목은 구현하지 않아도 된다는 것을 의미하는 것은 아니다. 담당자는 보안통제 항목의 선택 및 구현 방안에 대해 신중히 결정하여야 하며, 특히 새로운 정보서비스 모델을 구축하거나 여러 정보서비스 모델을 동시에 구축하고자 할 경우, 제안된 보안위협 외에 다양한 보안위협을 추가로 고려하여 보안통제 항목을 폭넓게 검토하고 보안대책을 수립하는 것이 필요하다.

담당자는 2장 1절에서와 같이 각급기관이 운영하고자 하는 정보서비스를 간단히 정의한 후, 2절 1항에서와 같이 준비 단계의 일환으로 정보서비스 구성요소 등을 분석(「활동-1-5」)할 수 있다.

또한, 2절의 위협 식별 단계 중 모델링 및 C/S/O 평가(「활동-3-1」), 보안원칙 적용(「활동-3-2」) 활동에서 어떤 원칙에 위배될 수 있는지를 파악하고 보안위협 식별(「활동-3-3」) 활동에서 기관 네트워크 환경구성 및 보안통제 적용 구조 등을 고려하여 제시되어 있는 보안 위협 외에 추가 보안위협에 대해 분석하여야 한다.

3절에서 제시된 보안대책 수립 단계에서는 상기 위협을 바탕으로 보안 요구사항 도출(「활동-4-1」) 활동을 진행하게 되는데 앞서 추가로 제시된 위협 및 기관 네트워크 환경구성, 관련 규정 등을 고려하여 보안 요구사항을 최종적으로 도출한다. 보안통제 선택(「활동-4-2」) 활동에서는 필요시 기존에 제시된 보안통제 항목 외에 추가로 보안통제 항목을 선택하거나 제시된 보안통제 항목을 수정·삭제하는 등 세부사항을 조정하는 것이 가능하다.

제2장

업무환경에서 생성형 AI 활용

제1절

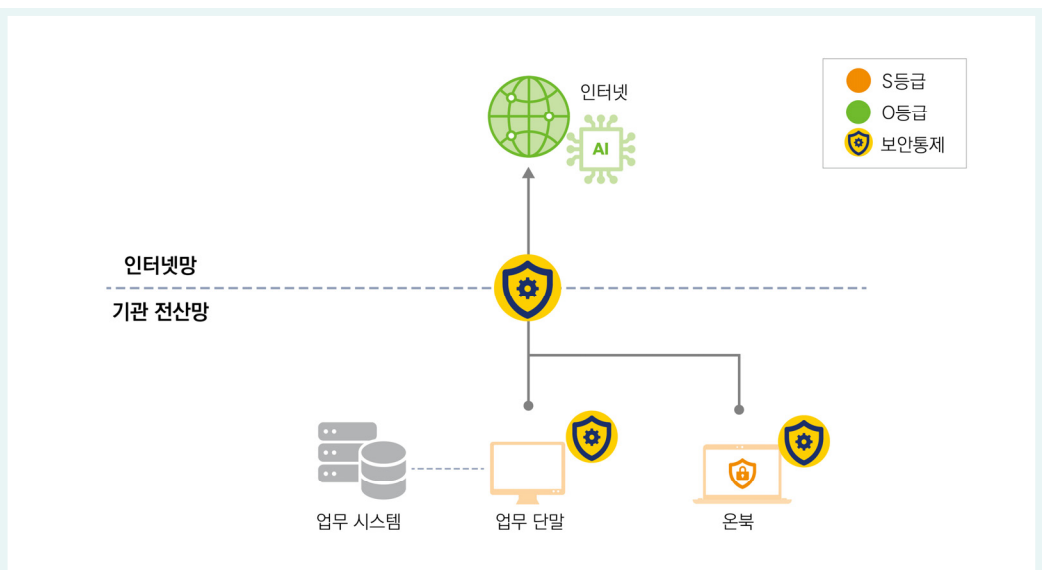
정보서비스 개요

본 정보서비스 모델에서는 업무 효율성 향상을 위해 이용자 단말에서 상용 생성형 AI 서비스(이하 생성형 AI 서비스)를 활용하기 위한 보안 요구사항 및 대책을 제시한다.

1절은 국가 망 보안체계(N2SF) 도입에 따라 업무환경에서 생성형 AI를 활용하는 정보서비스 변화를 보여주고, 2절은 정보서비스 환경에 맞춰 구성요소 분석, 모델링 및 보안등급 평가, 보안원칙 적용을 통한 보안위협 식별 절차를 수행한다. 3절은 보안위협에 대응하기 위한 필수 보안 요구사항과 보안통제 항목을 적용한 보안대책을 기술한다.

본 장에서는 국가 망 보안체계(N2SF)「업무환경에서 생성형 AI 활용」모델에 범용적으로 적용할 수 있는 정보서비스 위협식별 및 보안대책을 제시하고 있으며, 기관 환경 및 특성에 따라 추가적인 방안을 적용할 수 있다.

그림 2-1 업무환경에서 생성형 AI 활용 정보서비스 개요



제2절

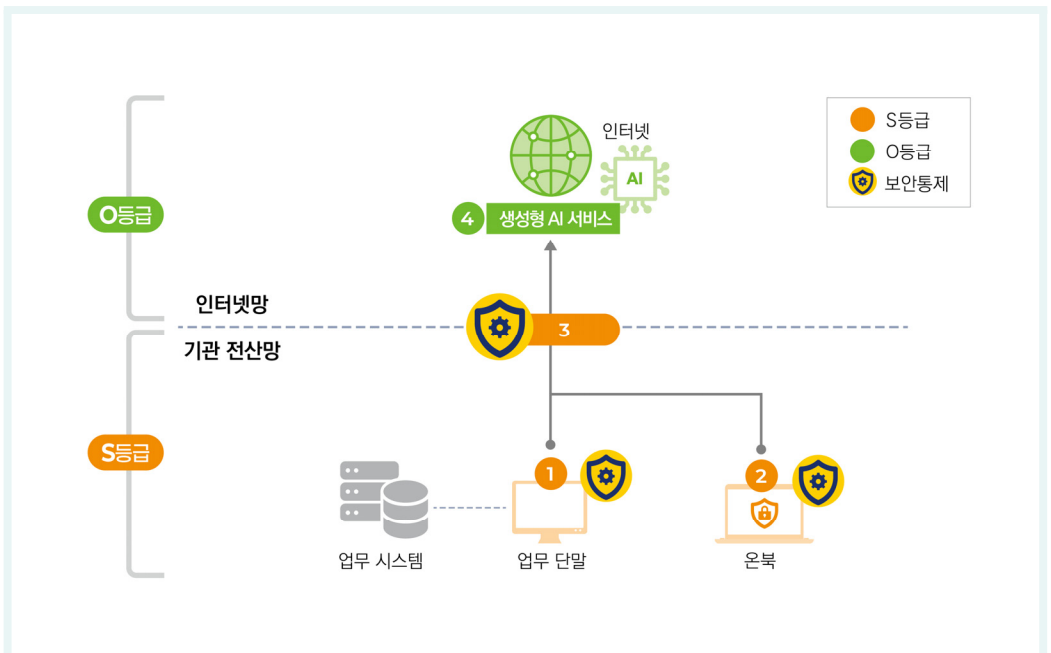
정보서비스 보안위협 식별

1. 정보서비스 구성요소 분석

본 정보서비스 모델은 기관 전산망 내 이용자 단말(업무 단말, 온북 등)을 통해 업무시스템에 접속하여 업무를 수행하는 환경에서, 업무 효율성 향상을 위해 인터넷 영역에 위치하는 생성형 AI 서비스를 활용하는 모델이다.

본 정보서비스는 기관 전산망 영역(S등급)에 위치하는 업무시스템(S등급), 이용자 단말(S등급)과 인터넷 영역(O등급)에 위치하는 생성형 AI 서비스(O등급)로 구성되며, 생성형 AI 서비스를 활용하는 업무정보는 O등급으로 한정한다.

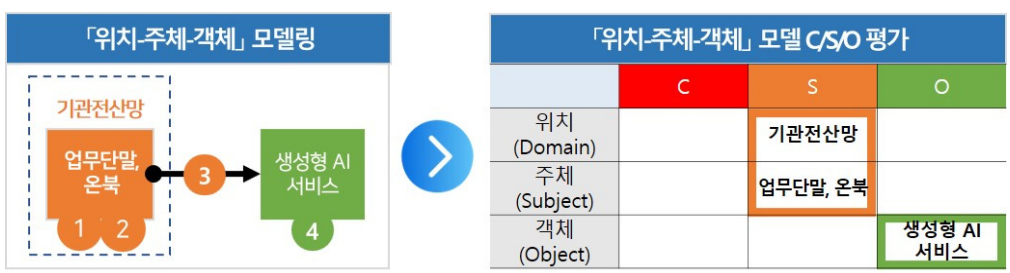
그림 2-2 정보서비스 구성요소 분석



2. 모델링 및 C/S/O 평가

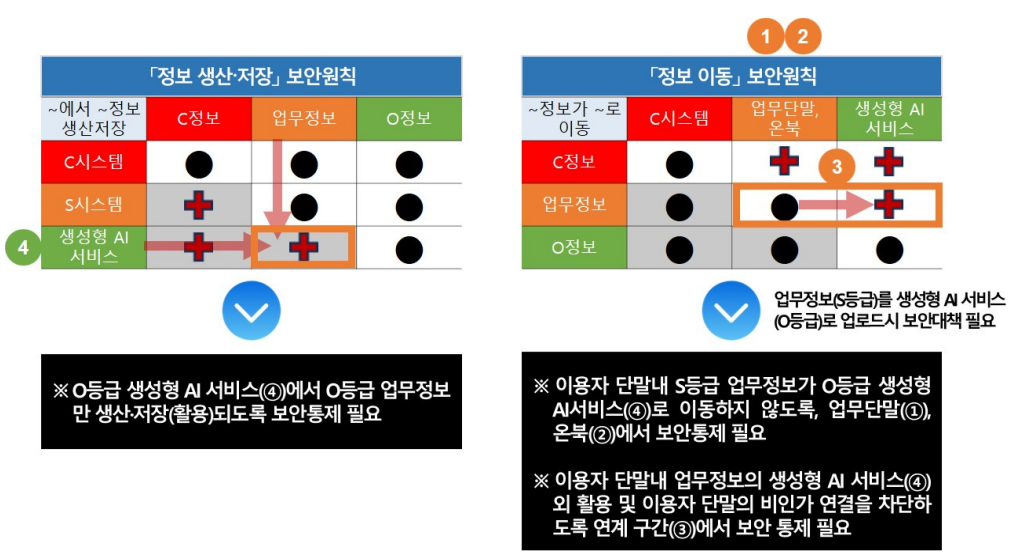
기관 전산망 내 이용자 단말에서 생성형 AI 서비스를 활용하는 정보서비스는 「위치(기관 전산망)-주체(이용자 단말: 업무 단말, 온북)-객체(생성형 AI 서비스)」로 모델링 할 수 있고, 이때 보안등급은 위치 S등급, 주체 S등급 및 객체 O등급으로 평가한다.

그림 2-3 「위치-주체-객체」 모델링 및 C/S/O 평가



3. 보안원칙 적용

그림 2-4 보안원칙 적용



가.「정보 생산·저장」 보안원칙 적용

기관 전산망 S등급 영역에 위치한 이용자 단말(업무 단말, 온북)은 모두 S등급이며, 이용자 단말에서 S등급, O등급 업무정보의 작성 및 보관은「정보 생산·저장」 보안원칙에 위배되지 않는다.

그러나, O등급의 생성형 AI 서비스에서 O등급 보다 상위의 업무정보를 생산하는 것은「정보 생산·저장」 보안원칙에 위배된다. 따라서, O등급 업무정보만 생성형 AI 서비스를 활용할 수 있도록 보안통제를 적용해야 한다.

나.「정보 이동」 보안원칙 적용

기관 전산망 S등급 영역에 위치한 이용자 단말(업무 단말, 온북)은 모두 S등급이며, 인터넷에 위치한 생성형 AI 서비스는 O등급이다.

생성형 AI 서비스 활용을 위해 이용자 단말 내 O등급 업무정보를 전송하는 것은「정보 이동」 보안원칙에 위배되지 않는다. 하지만, 이용자 단말 내 S등급 업무정보를 생성형 AI 서비스로 전송하는 것은「정보 이동」 보안원칙에 위배되므로, S등급 업무정보의 생성형 AI 서비스 전송에 대한 보안통제를 적용해야 한다.

그리고, 생성형 AI 서비스에서 생성한 O등급 정보를 이용자 단말로 이동하는 것은「정보 이동」 보안원칙에 위배되지 않으므로, 생성형 AI 서비스 생성 정보를 이용자 단말로 전송할 수 있다. 단, 기관 환경 및 특성에 따라 생성형 AI 서비스 생성 정보의 이동·활용 시 추가적인 보안통제를 적용할 수 있다.

또한, 이용자 단말 내 업무정보가 승인받은 생성형 AI 외 비인가 시스템으로 전송되거나, 이용자 단말과 외부와의 비인가 연결 차단, 외부로부터의 비인가 접근 차단 등을 위해 연계 구간에 대한 보안통제를 적용해야 한다.

4. 보안위협 식별

본 정보서비스 모델은 이용자 단말(①업무 단말, ②온북), AI 서비스 접근 제어를 위한 ③AI 연계체계, 업무환경에서 활용을 위한 ④생성형 AI 서비스로 구성되며, 〈표 2-1〉과 같이 정보서비스 모델 구성 대상별 보안위협을 식별한다.

그림 2-5 **보안위협 대상 식별**

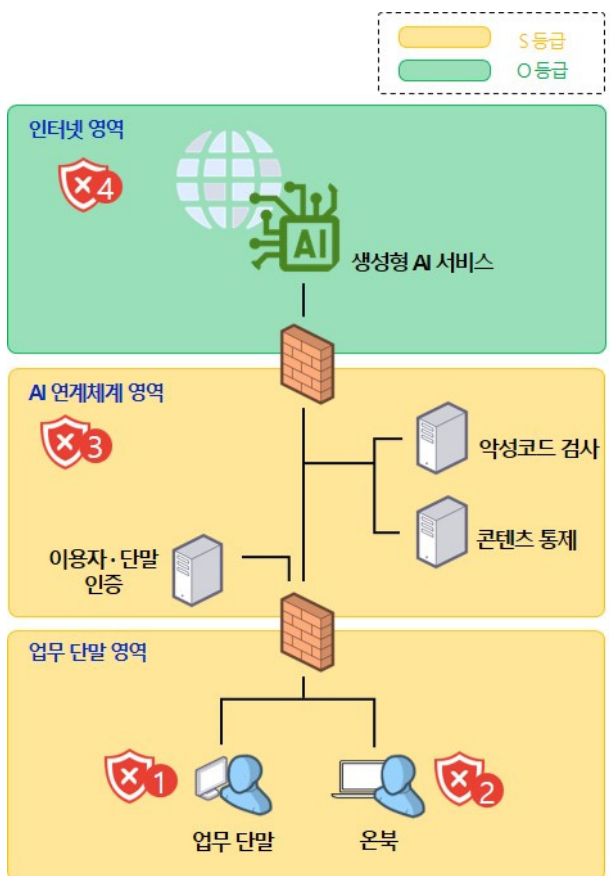


표 2-1 정보서비스 보안위협

대상	구분	보안위협 번호	보안위협
이용자 단말	① 업무 단말 ② 온북	TH-M2-1	단말 OS 및 SW 취약점 노출
		TH-M2-2	비인가 SW 설치·실행
		TH-M2-3	단말 비인가 사용
		TH-M2-4	비인가 네트워크 연결
		TH-M2-5	업무정보 비인가 유출
		TH-M2-6	AI 서비스 계정 정보를 통한 단말, 업무시스템 등 관련 정보 노출
		TH-M2-7	비인가 및 보안통제 미조치 단말의 생성형 AI 서비스 접근
		TH-M2-8	악성코드 유입 및 실행으로 인한 악성코드 감염
연계 체계	③ AI 연계 체계	TH-M2-9	이용자 단말의 AI 연계체계 비인가 접근
		TH-M2-10	이용자 단말의 AI 연계체계 우회 등 비인가 네트워크 연결
		TH-M2-11	사전 승인된 생성형 AI 서비스 외 접근
		TH-M2-12	공개(O) 등급 외 업무정보의 생성형 AI 서비스 활용
		TH-M2-13	생성형 AI 서비스 활용 시 계정 정보 등 송수신 데이터 유출
		TH-M2-14	외부로부터의 AI 연계체계 비인가 접근
		TH-M2-15	외부로부터의 악성 콘텐츠 유입
		TH-M2-16	AI 연계체계 관리자 계정 비인가 접근
		TH-M2-17	AI 연계체계 취약점 노출
		TH-M2-18	사전 승인된 생성형 AI 서비스 접속 실패
		TH-M2-19	AI 연계체계 운용 장애
서비스	④ 생성형 AI	TH-M2-20	비인가자의 기관 생성형 AI 서비스 계정 도용
		TH-M2-21	생성형 AI 서비스를 통한 업무정보 유출

제3절

보안 요구사항 및 보안대책

기관은 국가 망 보안체계(N2SF) 정보서비스 모델의 안전한 활용을 위해 「정보 생산·저장」 및 「정보 이동」 보안원칙을 준수해야 하며, 정보서비스 모델 구성요소 및 연계 지점에서 보안위협을 식별하고 이에 대한 보안대책을 적용해야 한다.

정보서비스 구성요소 분석, 모델링 및 C/S/O 평가, 보안원칙 적용, 보안위협 식별의 과정을 거쳐 식별한 위협에 대한 보안대책 수립 방향성 및 국가·공공기관의 정책적 요구사항을 반영하여 보안 요구사항을 도출하고, 보안 요구사항을 만족하는 N2SF 보안통제 항목을 선정하였다.

표 2-2 보안 요구사항 및 보안통제 항목

구분(유형)	구성요소	보안위협	보안 요구사항	N2SF 보안통제 항목
이용자 단말	① 업무 단말 ② 온북	(TH-M2-1) 단말 OS 및 SW 취약점 노출 (TH-M2-2) 비인가 SW 설치·실행 (TH-M2-8) 악성코드 유입 및 실행으로 인한 악성코드 감염	이용자 단말 보안성 유지	N2SF-LP-1 N2SF-DA-1 N2SF-DA-2 N2SF-DV-12 N2SF-IN-1(1) N2SF-IN-5 N2SF-IN-6 N2SF-IN-8 N2SF-IN-10 N2SF-IN-16
		(TH-M2-3) 단말 비인가 사용	이용자 단말 사용 보안	N2SF-AM-2 N2SF-AM-9 N2SF-DV-6 N2SF-DV-8
		(TH-M2-4) 비인가 네트워크 연결	이용자 단말 네트워크 보안	N2SF-SG-4 N2SF-SG-5 N2SF-SG-6 N2SF-IF-9 N2SF-EB-6 N2SF-SN-1 N2SF-WA-7 N2SF-BC-1 N2SF-DT-1

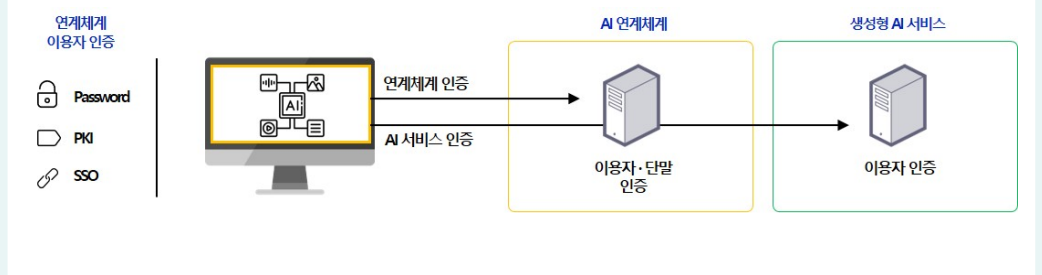
구분(유형)	구성요소	보안위협	보안 요구사항	N2SF 보안통제 항목
		(TH-M2-5) 업무정보 비인가 유출	이용자 단말 데이터 보호	N2SF-DU-2
		(TH-M2-6) AI 서비스 계정 정보를 통한 단말, 업무시스템 등 관련 정보 노출	이용자 계정 정보 보호	N2SF-IM-1
		(TH-M2-7) 비인가 및 보안통제 미조치 단말의 생성형 AI 서비스 접근	생성형 AI 서비스 활용 이용자 및 단말 관리	N2SF-LP-M1 N2SF-EB-M1 N2SF-DU-M3
연계 체계	③ AI 연계 체계	(TH-M2-9) 이용자 단말의 AI 연계체계 비인가 접근	생성형 AI 서비스 이용자 및 단말 인증	N2SF-AC-1 N2SF-AC-1(1) N2SF-AC-1(2) N2SF-AC-1(3) N2SF-AC-1(4) N2SF-AC-3 N2SF-AC-3(2) N2SF-DA-3 N2SF-DA-4 N2SF-LI-1 N2SF-LI-2 N2SF-LI-4
		(TH-M2-10) 이용자 단말의 AI 연계체계 우회 등 비인가 네트워크 연결 (TH-M2-11) 사전 승인된 생성형 AI 서비스 외 접근	비인가 네트워크 연결 차단	N2SF-IS-4 N2SF-IF-1 N2SF-IF-9 N2SF-EB-1 N2SF-EB-2 N2SF-EB-3 N2SF-EB-5 N2SF-EB-6 N2SF-EB-14 N2SF-EB-15
		(TH-M2-12) 공개(O) 등급 외 업무정보의 생성형 AI 서비스 활용 (TH-M2-13) 생성형 AI 서비스 활용 시 계정 정보 등 송수신 데이터 유출	생성형 AI 서비스 활용 시 데이터 보호	N2SF-IF-2 N2SF-IF-6 N2SF-IF-7 N2SF-IF-8 N2SF-IF-10 N2SF-IF-14
		(TH-M2-14) 외부로부터의 AI 연계체계 비인가 접근 (TH-M2-15) 외부로부터의 악성 콘텐츠 유입	외부 비인가 접근 및 악성 콘텐츠 유입 차단	N2SF-IF-3 N2SF-IF-5

구분(유형)	구성요소	보안위협	보안 요구사항	N2SF 보안통제 항목
		(TH-M2-16) AI 연계체계 관리자 계정 비인가 접근 (TH-M2-17) AI 연계체계 취약점 노출	연계체계 보안성 유지	N2SF-LP-4 N2SF-LP-4(1) N2SF-LP-4(4) N2SF-AC-1(5) N2SF-AC-3(1) N2SF-EB-8 N2SF-EB-10 N2SF-EB-11 N2SF-EB-13 N2SF-DV-4 N2SF-DV-12 N2SF-IN-1(1) N2SF-IN-5 N2SF-IN-6 N2SF-IN-11
		(TH-M2-18) 사전 승인된 생성형 AI 서비스 접속 실패 (TH-M2-19) AI 연계체계 운용 장애	연계체계 운용 관리	N2SF-LP-M1 N2SF-LP-M2 N2SF-AC-1(2) N2SF-AC-M1 N2SF-AC-M2 N2SF-AC-M3 N2SF-LI-M1 N2SF-LI-M2 N2SF-IF-M1 N2SF-IF-M2 N2SF-IF-M3 N2SF-IF-M4 N2SF-IF-M5 N2SF-EB-M3 N2SF-EB-M4 N2SF-EB-M5
서비스	④ 생성형 AI	(TH-M2-20) 비인가자의 기관 생성형 AI 서비스 계정 도용	생성형 AI 서비스 계정 관리	N2SF-EI-M1
		(TH-M2-21) 생성형 AI 서비스를 통한 업무정보 유출	생성형 AI 서비스 활용 데이터 관리	N2SF-DU-M3

1. 이용자 단말

이용자 단말(업무 단말, 온북)이 생성형 AI 서비스를 활용하기 위해서는 AI 연계체계를 통한 이용자·단말 인증 및 단말 보안통제가 적용되어야 한다. 다음은 이용자 단말에 적용해야 할 보안 요구사항 및 보안대책이다.

그림 2-6 이용자 및 단말 인증 절차



이용자 단말(업무 단말, 온북)은 인증·통제 서버를 이용하여 인증 및 보안 조치가 완료된 단말로 다음과 같은 보안 요구사항 및 생성형 AI 서비스에 접속하기 위한 브라우저 등 SW 활용을 고려해야 한다. 또한, 기관 환경 및 특성을 반영하여 추가적인 보안통제 적용·조정 등을 고려해야 한다.

그림 2-7 이용자 단말 사용 시나리오(예)

① 이용자 단말 보안성 유지

이용자 단말의 운영체제 및 설치되어 있는 소프트웨어의 취약점으로 인해 보안위협이 발생하지 않도록 최신 보안 업데이트 등 보안성을 유지해야 한다.

이용자 단말에 비인가 소프트웨어 설치·실행 및 단말 형상 비인가 변경으로 인한 보안위협이 발생하지 않도록 단말 소프트웨어 형상관리 등을 수행해야 한다.

이용자 단말에 악성코드가 유입·실행되어 감염으로 인한 보안위협이 발생하지 않도록 조치하여 보안성을 유지해야 한다.

그 외 기관 업무환경에 필요한 이용자 단말 보안 조치가 완료되어야 한다.

② 이용자 단말 사용 보안

비인가자의 단말 사용 등을 차단하기 위해 이용자 단말 부팅·사용 및 일정 시간 이상 단말 미사용 시 사용자 인증 등을 통해 단말을 사용할 수 있도록 보안 조치를 수행해야 한다.

③ 이용자 단말 네트워크 보안

이용자 단말의 안전한 생성형 AI 서비스 활용을 위해 네트워크 영역 및 단말 IP 관리 등을 수행해야 한다.

이용자 단말 내 업무정보의 네트워크를 통한 유출을 방지하기 위해 비인가 네트워크 연결 및 무선랜, 블루투스 등 비승인 네트워크 장치 사용 등을 차단해야 한다.

이용자 단말로부터 악성코드 전파, 다른 단말 및 정보시스템 비인가 접근 등을 차단하기 위한 네트워크 보안 조치를 수행해야 한다.

이용자 단말의 생성형 AI 서비스 등 업무 종료 시 네트워크 세션 처리 등을 수행해야 한다.

④ 이용자 단말 데이터 보호

이용자 단말 내 업무정보 무단 이동, 복사 등을 방지하기 위한 데이터 보호 조치를 적용해야 한다.

⑤ 이용자 계정 정보 보호

업무시스템 계정 정보와의 혼재 및 계정 탈취·오용 등을 방지하기 위해 생성형 AI 서비스의 이용자 계정 정보는 기관 업무시스템 계정 정보와 분리하여 관리해야 한다.

⑥ 생성형 AI 서비스 활용 이용자 및 단말 관리

생성형 AI 서비스 활용을 위한 이용자 단말 사전 승인 등 관리 절차를 수립해야 한다.

생성형 AI 서비스 활용을 위한 데이터 사용 정책 등을 수립해야 한다.

기관은 위와 같은 보안 요구사항을 고려하여 〈표 2-3〉의 보안통제 항목을 포함하는 보안대책을 준수해야 한다.

표 2-3 이용자 단말(업무 단말, 온북) 보안통제 항목

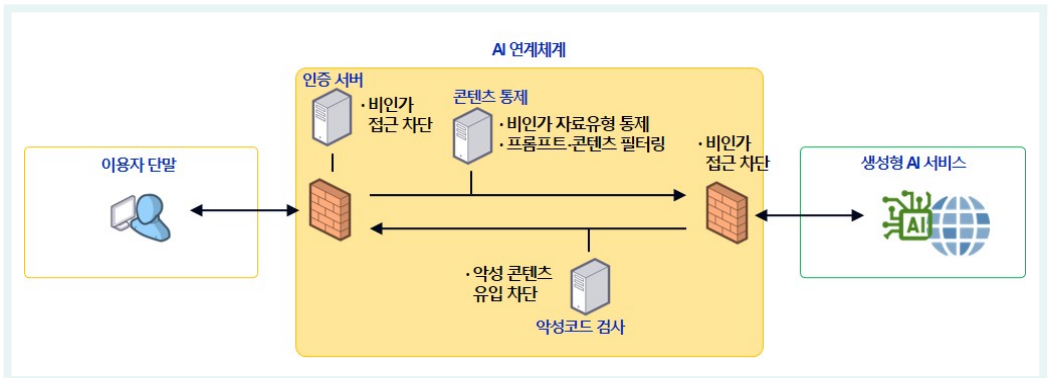
코드	보안통제 항목	내용
① 이용자 단말 보안성 유지		
N2SF-LP-1	정보시스템 접근 권한 정의	• 업무정보(데이터)를 식별하고, 업무정보를 저장하고 있는 정보시스템 접근 권한을 정의한다.
N2SF-DA-1	단말 무결성 검증	• 단말 내 신뢰 가능한 모듈(TPM 등)을 통한 구성정보(BIOS 설정정보, Disk 설치 정보 등) 등을 확인한다.
N2SF-DA-2	정보서비스 식별 및 제한	• 인증절차를 통해 사전 승인한 정보서비스만을 활용하도록 제한한다.
N2SF-DV-12	장치 펌웨어 업데이트 검증	• 펌웨어 업데이트 시 서명 검증 또는 위변조 여부를 검증하여 설치를 제한한다.
N2SF-IN-1(1)	정보시스템 구성요소 최신상태 유지	• 정보시스템 내의 모든 구성요소가 포함되도록 정보시스템 구성요소 목록을 작성하고 정기적으로 검토 및 최신 상태로 업데이트 한다.
N2SF-IN-5	비인가 변경 방지	• 인가되지 않은 정보시스템 구성요소 변경을 방지한다.
N2SF-IN-6	불필요한 구성요소 제거	• 필요 기능만 제공하도록 구성하고, 사용하지 않는 기능, 포트, 프로토콜, 소프트웨어, 서비스의 사용을 제거하거나 비활성화한다.
N2SF-IN-8	비인가 소프트웨어 실행 차단	• 허가되지 않은 소프트웨어(응용프로그램)가 실행되지 않도록 차단한다.
N2SF-IN-10	소프트웨어 설치 권한 제한	• 소프트웨어 설치 권한은 필요한 사용자에게만 부여한다.
N2SF-IN-16	악성코드 감염 차단	• 악성코드 유입 및 실행 등으로 인한 악성코드 감염을 실시간 탐지하고 차단한다.
② 이용자 단말 사용 보안		
N2SF-AM-2	비밀번호 기반 인증	• 숫자•문자•특수문자 등을 혼합하고 주기적으로 변경하는 비밀번호 인증체계를 적용한다.
N2SF-AM-9	소유기반 인증	• 생체인증, 모바일 인증 및 하드웨어 토큰 등을 활용한 인증체계를 적용한다.
N2SF-DV-6	통신 기능이 포함된 저장장치 제한	• 통신기능이 포함된 저장장치를 사용을 제한한다.
N2SF-DV-8	장치 자동 잠금	• 사용자가 일정시간 이상 정보시스템을 사용하지 않거나 방치할 경우 잠금 기능을 활성화하고, 화면에 표시되는 정보는 표출되지 않아야 한다.

코드	보안통제 항목	내용
③ 이용자 단말 네트워크 보안		
N2SF-SG-4	IP체계	• 서로 다른 영역 또는 정보자산(기능 등)별IP체계를 분리하고, 보안통제를 적용한다.
N2SF-SG-5	보안•운영관리 인프라 분리	• 보안•운영관리 인프라를 물리적으로 분리된 네트워크로 구성하여 이외 정보시스템과 분리한다.
N2SF-SG-6	보안 기능과 사용자 기능 분리	• 인증, 감사 및 데이터 통제와 같은 핵심 보안 기능과 데이터 입력, 애플리케이션 실행 등 사용자 기능을 분리한다.
N2SF-IF-9	출발지점과 도착지점 식별 및 인증	• 정보 전송 시 개인, 기관, 응용프로그램 혹은 정보시스템 등 하나 이상을 사용하여 출발지점과 도착지점을 식별하고 인증한다.
N2SF-EB-6	외부로의 사이버위협 통신 발신 제한	• 내부에서 외부 네트워크에 사이버위협을 가하는 발신(outbound) 통신을 탐지 및 차단하고, 발신자(사용자 및 정보자산 등)를 식별한다.
N2SF-SN-1	로그아웃 세션 처리	• 로그아웃 또는 비정상 세션 종료 시 연결되었던 모든 세션의 식별자를 즉시 무효화하며, 더 이상 세션이 유효하지 않도록 한다.
N2SF-WA-7	비인가 무선망 접속 차단	• 인가되지 않은 무선망 접속을 차단한다.
N2SF-BC-1	블루투스 데이터 통신 제한	• 블루투스 장치 연결 시 키보드, 마우스, 오디오 등을 위한 입출력 기능 외 데이터 통신은 차단한다.
N2SF-DT-1	전송 권한 확인	• 데이터가 전송되기 전에 이를 처리하는 개인이나 정보시스템이 적절한 권한을 보유하고 있는지 확인한다.
④ 이용자 단말 데이터 보호		
N2SF-DU-2	데이터 암호화 저장	• 데이터 대상 암호기술을 적용하여 기밀성을 보장한다.
⑤ 이용자 계정 정보 보호		
N2SF-IM-1	공개된 식별자의 계정 사용 금지	• 정보시스템 계정 식별자로 개인의 공개된 식별자 사용을 금지한다.
⑥ 생성형 AI 서비스 활용 이용자 및 단말 관리		
N2SF-LP-M1	특별권한 사용자 지정	• 일반 사용 권한과 별도로 특별권한 사용자 그룹을 지정하고, 이들의 권한 부여와 변경을 통제한다.
N2SF-EB-M1	개인 식별정보 보호	• 외부와 통신 시 개인을 식별하거나 특정 개인과 관련된 정보를 포함하는 경우 노출되지 않도록 조치한다.
N2SF-DU-M3	데이터 사용 정책 수립	• 데이터의 사용 목적, 접근 권한, 보존 기간, 폐기 절차 등을 포함하는 데이터 사용 정책을 문서화하고 전사적으로 적용 및 관리한다.

2. 연계체계

이용자 단말(업무 단말, 온북)은 AI 연계체계를 통해 생성형 AI 서비스를 활용할 수 있으며, 다음과 같이 보안 요구사항 및 보안대책을 적용해야 한다.

그림 2-8 AI 연계체계



이용자 단말(업무 단말, 온북)의 생성형 AI 서비스 이용을 위해 구성되는 AI 연계체계는 다음과 같은 보안 요구사항을 고려해야 한다. 또한, 기관 환경 및 특성을 반영하여 추가적인 보안통제 적용·조정 등을 고려해야 한다.

① 생성형 AI 서비스 이용자 및 단말 인증

이용자 및 단말의 생성형 AI 서비스 연계를 위한 인증을 수행해야 하며, 인증 과정에서 사용자 및 단말 정보가 노출되지 않도록 보안통제를 적용해야 한다.

생성형 AI 서비스 활용 시 의심스러운 활동 및 일정 시간 이상 비활동인 계정에 대한 보안조치를 적용해야 한다.

일정 횟수 이상 인증 실패에 대한 보호조치 및 잠금 해제 대책을 적용해야 한다.

② 비인가 네트워크 연결 차단

이용자 단말의 AI 연계체계 우회 시도 및 사전 승인된 생성형 AI 서비스 외 비인가 네트워크로의 접근을 차단해야 한다.

AI 연계체계를 통해 이용자 단말과 생성형 AI 서비스의 통신을 연계해야 하며, 기관 전산망과 생성형 AI 서비스가 직접 연결되지 않도록 네트워크 격리 등 보안대책을 적용해야 한다.

비인가 네트워크 프로토콜은 차단해야 한다.

③ 생성형 AI 서비스 활용 시 데이터 보호

AI 연계체계를 통해 생성형 AI 서비스 활용 시 프롬프트·콘텐츠 필터링, 보안등급 식별 등을 통해 승인된 공개(O) 등급 외 업무정보가 유출되지 않도록 보호조치를 적용해야 한다.

생성형 AI 서비스 활용 시 기관이 사전 정의한 정보 전송 방식 및 데이터 유형만 활용할 수 있도록 데이터 보호조치를 적용해야 한다.

④ 외부 비인가 접근 및 악성 콘텐츠 유입 차단

AI 연계체계는 이용자 단말에서 생성형 AI 서비스로의 일방향 정보흐름만 허용하도록 통제해야 하며, 외부로부터 AI 연계체계의 비인가 접근을 차단해야 한다.

AI 연계체계를 통해 전달되는 콘텐츠를 통해 악성코드가 전달되지 않도록 통제해야 한다.

⑤ 연계체계 보안성 유지

AI 연계체계 관리자 권한 계정을 일반 사용자 계정과 분리하여 관리해야 하며, 비인가 장치의 연결 등을 통제해야 한다.

AI 연계체계의 취약점으로 인해 보안위협이 발생하지 않도록 최신 보안 업데이트 등 보안성을 유지해야 한다.

그 외 기관 업무환경에 필요한 AI 연계체계의 보안 조치가 완료되어야 한다.

⑥ 연계체계 운용 관리

AI 연계체계 관리자 및 관리 단말 지정 등 운용 관련 체계를 수립해야 한다.

AI 연계체계 운용에 대한 감사 로그를 생성·관리하고, 이용자 단말 인증, 세션, 정보흐름 통제 등 관련 정보를 모니터링 해야 한다.

AI 연계체계 침해, 장애 등에 대한 대응체계 절차를 수립해야 한다.

기관은 위와 같은 보안 요구사항을 고려하여 〈표 2-4〉의 보안통제 항목을 포함하는 보안대책을 준수해야 한다.

표 2-4 AI 연계체계 보안통제 항목

코드	보안통제 항목	내용
① 생성형 AI 서비스 이용자 및 단말 인증		
N2SF-AC-1	계정 관리 자동화	• 정보시스템 계정 관리를 효율화하고, 인적 오류를 최소화하기 위해 자동화된 메커니즘을 사용하여 계정 관리를 수행한다.
N2SF-AC-1(1)	동적 계정 관리	• 사용자 상태(입사, 퇴사, 부서 이동 등)에 따라 계정 정보를 실시간으로 반영하고, 시스템 간 계정 동기화를 통해 계정 수명주기 관리를 자동화한다.
N2SF-AC-1(2)	계정 상태 모니터링	• 계정의 임시 생성, 수정, 활성화, 비활성화 및 삭제 등을 모니터링한다.
N2SF-AC-1(3)	계정 자동 비활성화	• 계정 사용 기간이 종료되거나 일정 기간 미사용된 계정은 자동으로 비활성화한다.
N2SF-AC-1(4)	계정 자동 로그아웃	• 비활동 시간이 일정 기간 지속되었을 때 정보시스템에서 자동 로그아웃 되어야 한다.
N2SF-AC-3	의심스러운 계정 모니터링	• 비정상적이거나 의심스러운 계정 접속 시도 및 활동을 지속적으로 모니터링한다.
N2SF-AC-3(2)	내부 사용자 모니터링	• 내부 사용자의 계정 사용 및 활동을 지속적으로 모니터링한다.
N2SF-DA-3	단말 식별 및 인증	• 단말의 고유 식별자(MAC, TPM, 인증서 등)를 통해 단말을 식별하고, 등록된 단말만 인증을 통해 시스템에 접근할 수 있도록 한다.
N2SF-DA-4	인증된 단말의 접속 관리	• 인증된 단말이라 하더라도 접속 시간, 위치, 사용자에 따라 세부 접근 권한을 제어하고, 접근 이력을 기록하여 감사 가능하도록 한다.
N2SF-LI-1	유효한 인증정보 노출 방지	• 인증 과정에서 유효한 인증 정보가 노출되지 않도록 한다.
N2SF-LI-2	로그인 실패에 따른 접속 제한	• 정의한 횟수 이상 연속적으로 로그인을 실패한 경우 일정시간 계정을 차단(또는 잠김)하거나 접속을 제한한다.
N2SF-LI-4	계정 잠금 해제 인증요소 추가	• 계정 잠금 상태에서 해제 요청 시 기본 인증 요소 외 인증요소를 추가 사용한다.
② 비인가 네트워크 연결 차단		
N2SF-IS-4	네트워크 격리	• 내부망, 외부망, 보안망 등 네트워크 간에 방화벽, 라우팅 제어 등으로 트래픽을 분리하여 정보 유출 또는 확산을 방지한다.
N2SF-IF-1	정보흐름의 동적 통제	• 정보시스템의 비정상 동작, 외부의 공격 등 지정한 조건에 대하여 정보흐름을 동적으로 통제한다.
N2SF-IF-9	출발지점과 도착지점 식별 및 인증	• 정보 전송 시 개인, 기관, 응용프로그램 혹은 정보시스템 등 하나 이상을 사용하여 출발지점과 도착지점을 식별하고 인증한다.

코드	보안통제 항목	내용
N2SF-EB-1	연결 접점 제한	• 정보시스템의 외부 네트워크 연결 접점 수를 제한한다.
N2SF-EB-2	서비스별 외부 통신 통제	• 외부와 통신하는 서비스의 경계마다 통신흐름을 통제한다.
N2SF-EB-3	화이트리스트 기반 통신 허용	• 기본적으로 모든 통신을 차단한 상태에서 필요한 통신만을 허용하는 화이트리스트 기반 정책을 적용한다.
N2SF-EB-5	통신 경유(proxy) 강제화	• 인가된 정보시스템을 경유하여 통신하도록 통신경로를 강제화한다.
N2SF-EB-6	외부로의 사이버위협 통신 발신 제한	• 내부에서 외부 네트워크에 사이버위협을 가하는 발신(outbound) 통신을 탐지 및 차단하고, 발신자(사용자 및 정보자산 등)를 식별한다.
N2SF-EB-14	외부 DNS 통신 제한	• 인가된 DNS 서버 외의 요청을 차단한다.
N2SF-EB-15	우회 통신 수단 탐지 및 차단	• VPN, Tor 등 우회 경로 사용을 탐지하고 차단한다.
③ 생성형 AI 서비스 활용 시 데이터 보호		
N2SF-IF-2	암호화된 정보흐름 통제	• 암호화된 정보의 내용을 확인하기 위하여 정보를 복호화하거나, 확인이 불가능한 암호화된 정보는 흐름을 차단하는 등의 조치를 적용한다.
N2SF-IF-6	필터링 규칙 정보흐름 통제	• 보안 및 프라이버시 등에 관한 필터링 규칙을 적용하여 정보흐름을 통제한다.
N2SF-IF-7	데이터 유형 식별자 통제	• 서로 다른 영역 간에 정보를 전송하는 경우 데이터 유형 식별자를 확인하여 전송 여부를 통제한다.
N2SF-IF-8	인가되지 않은 정보 전송 통제	• 인가되지 않은 정보가 포함되었는지 검사하고 보안정책에 따라 해당 정보의 전송을 차단한다.
N2SF-IF-10	정보 전송 방식 제한	• 정보 전송 시 특정 매체나 방식만 허용하고 나머지는 차단한다.
N2SF-IF-14	보안등급 기반 흐름 통제	• 보안등급에 따라 정보 흐름을 제한하여 상위 등급에서 하위 등급으로의 부적절한 전송을 차단한다.
④ 외부 비인가 접근 및 악성 콘텐츠 유입 차단		
N2SF-IF-3	임베디드 데이터 삽입 차단	• 임베이드된 데이터 내부에 인가되지 않은 다른 종류의 데이터가 삽입되는 것을 차단한다.
N2SF-IF-5	일방향 정보흐름 통제	• 일방향 전송 장치를 통해 단방향 정보 흐름만 허용하고 반대 방향 흐름을 차단한다.
⑤ 연계체계 보안성 유지		
N2SF-LP-4	관리자 권한 제한	• 정보시스템 접근에 필요한 최소한의 관리자 및 운영자 등에게만 관리자 권한을 부여한다.

코드	보안통제 항목	내용
N2SF-LP-4(1)	원격접속을 통한 관리자 권한 접속제한	• 기관 네트워크 내부에서 관리자 권한 접속이 제한되는 경우 등 불가피한 상황에서만 한시적으로 기관 네트워크 외부에서의 관리자 권한 접속을 허용하며, 목적이 달성된 경우 외부에서의 관리자 권한 접속을 즉시 차단한다.
N2SF-LP-4(4)	관리자 권한 실행 로깅 및 감사	• 관리자 권한 기능 실행 내역은 로깅하고 주기적인 사용 내역 감사를 실시한다.
N2SF-AC-1(5)	불필요한 관리자 권한 계정 제거	• 관리자 권한이 필요 없거나 활용이 종료된 계정은 비활성화 또는 삭제 조치한다.
N2SF-AC-3(1)	위험에 노출된 계정 비활성화	• 정보시스템 위협 탐지 시, 위협에 노출된 계정은 신속히 비활성화하거나 제한 조치를 한다.
N2SF-EB-8	운영관리용 포트의 물리적 연결 차단	• 운영관리용 포트에 인가되지 않은 장치의 포트 연결을 차단한다.
N2SF-EB-10	정보시스템 구성요소 외부 노출 차단	• 정보시스템 운영관리 및 서비스를 제공하는 구성요소가 외부 노출되지 않도록 차단한다.
N2SF-EB-11	외부 경계 보호 기능 유지	• 외부 경계를 보호하는 정보자산(보안시스템 등) 장애 시에도 보호기능은 유지되도록 구성한다.
N2SF-EB-13	오류정보 발신자 전송 제한	• 네트워크 규약에 따른 통신 오류 발생 시 발신자에게 피드백이나 경고를 통해 정보시스템 구성이나 취약점이 전송되지 않도록 한다.
N2SF-DV-4	포트 및 입출력 장치 제어	• 정보시스템의 포트나 입출력 장치를 제어하여 악성코드 유입 및 정보 유출을 차단한다.
N2SF-DV-12	장치 펌웨어 업데이트 검증	• 펌웨어 업데이트 시 서명 검증 또는 위변조 여부를 검증하여 설치를 제한한다.
N2SF-IN-1(1)	정보시스템 구성요소 최신상태 유지	• 정보시스템 내의 모든 구성요소가 포함되도록 정보시스템 구성요소 목록을 작성하고 정기적으로 검토 및 최신 상태로 업데이트 한다.
N2SF-IN-5	비인가 변경 방지	• 인가되지 않은 정보시스템 구성요소 변경을 방지한다.
N2SF-IN-6	불필요한 구성요소 제거	• 필요 기능만 제공하도록 구성하고, 사용하지 않는 기능, 포트, 프로토콜, 소프트웨어, 서비스의 사용을 제거하거나 비활성화한다.
N2SF-IN-11	재기동 서비스 신뢰성 확보	• 정보시스템 구성요소와 서비스가 재기동(재부팅) 할 때 소프트웨어와 데이터는 신뢰된 곳으로부터 획득한다.
⑥ 연계체계 운용 관리		
N2SF-LP-M1	특별권한 사용자 지정	• 일반 사용 권한과 별도로 특별권한 사용자 그룹을 지정하고, 이들의 권한 부여와 변경을 통제한다.
N2SF-LP-M2	주요 사용자 위험 관리	• 주요 사용자의 권한과 활동을 모니터링하고 이상 징후를 탐지하여 위험을 사전에 관리한다.

코드	보안통제 항목	내용
N2SF-AC-1(2)	계정 상태 모니터링	• 계정의 임시 생성, 수정, 활성화, 비활성화 및 삭제 등을 모니터링한다.
N2SF-AC-M1	감사 활동 자동화	• 계정 사용 및 관련된 감사 활동을 자동화하여 관리
N2SF-AC-M2	감사기록 생성	• 계정 활동에 대한 감사 기록을 생성하여 보관 및 분석할 수 있도록 함
N2SF-AC-M3	세션 감사	• 세션 활동을 기록하고 주기적으로 감사하여 비정상적 행위 탐지
N2SF-LI-M1	로그인 실패 모니터링 및 보고	• 반복 실패, 의심 로그인 시도 등의 실패 패턴을 실시간 감지하고 관리자에게 보고
N2SF-LI-M2	주기적 로그인 정보 무결성 점검	• 로그인 관련 데이터(세션, 토큰, 사용자 매핑 정보 등)에 대해 주기적인 무결성 점검 및 이상 여부 확인
N2SF-IF-M1	정보흐름 통제 정책 수립 및 갱신	• 정보 흐름에 대한 통제 기준 및 예외 절차를 문서화하고 정기적으로 갱신한다.
N2SF-IF-M2	정보흐름 로그 기록 및 보존	• 정보 흐름 통제 활동(허용/차단 등)을 로깅하고, 법적/감사 목적으로 일정 기간 보관한다.
N2SF-IF-M3	정보흐름 통제 감사 및 이행 점검	• 정보 흐름 통제의 적용 현황을 정기적으로 점검하여 정책 미준수 사항 식별 및 개선
N2SF-IF-M4	비인가 흐름 탐지 자동화	• 정책을 우회하거나 비정상적 흐름을 탐지하기 위한 자동화 도구 또는 시스템 구축
N2SF-IF-M5	통제 실패·예외 보고 체계	• 통제가 실패하거나 예외 발생 시 담당자에게 자동 보고하고 이를 기록하는 체계를 마련한다.
N2SF-EB-M3	외부 통신 로그 기록 및 감사	• 외부 통신 활동과 설정 변경 사항을 기록하고 감사 가능하도록 조치
N2SF-EB-M4	외부 경계 위협 탐지 자동화	• 이상 행위를 자동으로 탐지하는 시스템을 운영한다.
N2SF-EB-M5	비상 시 외부 통신 격리	• 침해 발생 시 외부 통신을 즉시 차단할 수 있는 절차를 마련한다.

3. 생성형 AI 서비스

기관은 생성형 AI 서비스 활용 시 업무정보 유출, 계정 도용 등을 방지하기 위해 다음과 같은 보안 요구사항을 고려해야 한다.

그림 2-9 생성형 AI 서비스

① 생성형 AI 서비스 계정 관리

생성형 AI 서비스를 활용하는 기관 이용자는 계정의 임의 도용을 방지하기 위해 계정 관리를 위한 보안대책을 수립해야 한다.

② 생성형 AI 서비스 활용 데이터 관리

기관은 이용자가 생성형 AI 서비스 활용 시 허용되지 않은 업무정보가 유출되지 않도록 데이터 활용 정책을 수립해야 한다.

기관은 위와 같은 보안 요구사항을 고려하여 〈표 2-5〉의 보안통제 항목을 포함하는 보안대책을 준수해야 한다.

표 2-5 생성형 AI 서비스 활용 보안통제 항목

코드	보안통제 항목	내용
① 생성형 AI 서비스 계정 관리		
N2SF-EI-M1	외부 인증 수단 관리	• 외부 인증 수단의 등록, 변경, 폐지 등 전체 수명주기를 체계적으로 관리하며, 외부 기관과의 연계된 인증 프로파일의 보안 검증을 주기적으로 수행한다.
② 생성형 AI 서비스 활용 데이터 관리		
N2SF-DU-M3	데이터 사용 정책 수립	• 데이터의 사용 목적, 접근 권한, 보존 기간, 폐기 절차 등을 포함하는 데이터 사용 정책을 문서화하고 전사적으로 적용 및 관리한다.

1.0

국가 망 보안체계
보안 가이드라인

정보서비스 모델 해설서 모델 2. 업무환경에서 생성형 AI 활용

부록 2-2